LAWFARE

Toward an Information Operations Kill Chain

Bruce Schneier

Wednesday, April 24, 2019, 3:33 PM

Cyberattacks don't magically happen; they involve a series of steps. And far from being helpless, defenders can disrupt the attack at any of those steps. This framing has led to something called the "cybersecurity kill chain": a way of thinking about cyber defense in terms of disrupting the attacker's process.

Cyberattacks don't magically happen; they involve a series of steps. And far from being helpless, defenders can disrupt the attack at any of those steps. This framing has led to something called the "cybersecurity kill chain": a way of thinking about cyber defense in terms of disrupting the attacker's process.

On a similar note, it's time to conceptualize the "information operations kill chain." Information attacks against democracies, whether they're attempts to polarize political processes or to increase mistrust in social institutions, also involve a series of steps. And enumerating those steps will clarify possibilities for defense.

I first heard of this concept from Anthony Soules, a former National Security Agency (NSA) employee who now leads cybersecurity strategy for Amgen. He used the steps from the 1980s Russian "Operation Infektion," designed to spread the rumor that the U.S. created the HIV virus as part of a weapons research program. A 2018 New York Times opinion video series on the operation described the Russian disinformation playbook in a series of seven "commandments," or steps. The information landscape has changed since 1980, and information operations have changed as well. I have updated, and added to, those steps to bring them into the present day:

> **Step 1: Find the cracks** in the fabric of society—the social, demographic, economic and ethnic divisions.
>
> **Step 2: Seed distortion** by creating alternative narratives. In the 1980s, this was a single "big lie," but today it is more about many contradictory alternative truths—a "firehose of falsehood"—that distorts the political debate.
>
> **Step 3: Wrap those narratives in kernels of truth.** A core of fact helps the falsities spread.

Step 4: (This step is new.) **Build audiences**, either by directly controlling a platform (like RT) or by cultivating relationships with people who will be receptive to those narratives.

Step 5: Conceal your hand; make it seem as if the stories came from somewhere else.

Step 6: Cultivate "useful idiots" who believe and amplify the narratives. Encourage them to take positions even more extreme than they would otherwise.

Step 7: Deny involvement, even if the truth is obvious.

Step 8: Play the long game. Strive for long-term impact over immediate impact.

These attacks have been so effective in part because, as victims, we weren't aware of how they worked. Identifying these steps makes it possible to conceptualize—and develop—countermeasures designed to disrupt information operations. The result is the information operations kill chain:

Step 1: Find the cracks. There will always be open disagreements in a democratic society, but one defense is to shore up the institutions that make that society possible. Elsewhere I have written about the "common political knowledge" necessary for democracies to function. We need to strengthen that shared knowledge, thereby making it harder to exploit the inevitable cracks. We need to make it unacceptable—or at least costly—for domestic actors to use these same disinformation techniques in their own rhetoric and political maneuvering, and to highlight and encourage cooperation when politicians honestly work across party lines. We need to become reflexively suspicious of information that makes us angry at our fellow citizens. We cannot entirely fix the cracks, as they emerge from the diversity that makes democracies strong; but we can make them harder to exploit.

Step 2: Seed distortion. We need to teach better digital literacy. This alone cannot solve the problem, as much sharing of fake news is about social signaling, and those who share it care more about how it demonstrates their core beliefs than whether or not it is true. Still, it is part of the solution.

Step 3: Wrap the narratives in kernels of truth. Defenses involve exposing the untruths and distortions, but this is also complicated to put into practice. Psychologists have demonstrated that an inadvertent effect of debunking a piece of fake news is to amplify the message of that debunked story. Hence, it is essential to replace the fake news with accurate narratives that counter the propaganda. That kernel of truth is part of a

larger true narrative. We need to ensure that the true narrative is legitimized and promoted.

Step 4: Build audiences. This is where social media companies have made all the difference. By allowing groups of like-minded people to find and talk to each other, these companies have given propagandists the ability to find audiences who are receptive to their messages. Here, the defenses center around making disinformation efforts less effective. Social media companies need to detect and delete accounts belonging to propagandists and bots and groups run by those propagandists.

Step 5: Conceal your hand. Here the answer is attribution, attribution, attribution. The quicker we can publicly attribute information operations, the more effectively we can defend against them. This will require efforts by both the social media platforms and the intelligence community, not just to detect information operations and expose them but also to be able to attribute attacks. Social media companies need to be more transparent about how their algorithms work and make source publications more obvious for online articles. Even small measures like the Honest Ads Act, requiring transparency in online political ads, will help. Where companies lack business incentives to do this, regulation will be the only answer.

Step 6: Cultivate useful idiots. We can mitigate the influence of people who disseminate harmful information, even if they are unaware they are amplifying deliberate propaganda. This does not mean that the government needs to regulate speech; corporate platforms already employ a variety of systems to amplify and diminish particular speakers and messages. Additionally, the antidote to the ignorant people who repeat and amplify propaganda messages is other influencers who respond with the truth—in the words of one report, we must "make the truth louder." Of course, there will always be true believers for whom no amount of fact-checking or counter speech will convince; this is not intended for them. Focus instead on persuading the persuadable.

Step 7: Deny everything. When attack attribution relies on secret evidence, it is easy for the attacker to deny involvement. Public attribution of information attacks must be accompanied by convincing evidence. This will be difficult when attribution involves classified intelligence information, but there is no alternative. Trusting the government without evidence, as the NSA's Rob Joyce recommended in a 2016 talk, is not enough. Governments will have to disclose.

Step 8: Play the long game. Counterattacks can disrupt the attacker's ability to maintain information operations, as U.S. Cyber Command did during the 2018 midterm elections. The NSA's new policy of "persistent

engagement" (see the article by, and interview with, U.S. Cyber Command Commander's Gen. Paul Nakasone here) is a strategy to achieve this. Defenders can play the long game, too. We need to better encourage people to think for the long term: beyond the next election cycle or quarterly earnings report.

Permeating all of this is the importance of deterrence. Yes, we need to adjust our theories of deterrence to the realities of the information age and the democratization of attackers. If we can mitigate the effectiveness of information operations, if we can publicly attribute, if we can respond either diplomatically or otherwise—we can deter these attacks from nation-states. But Russian interference in the 2016 presidential election shows not just that such actions are possible but also that they're surprisingly inexpensive to run. As these tactics continue to be democratized, more people will attempt them. Deterring them will require a different theory.

None of these defensive actions is sufficient on its own. In this way, the information operations kill chain differs significantly from the more traditional cybersecurity kill chain. The latter defends against a series of steps taken sequentially by the attacker against a single target—a network or an organization—and disrupting any one of those steps disrupts the entire attack. The information operations kill chain is fuzzier. Steps overlap. They can be conducted out of order. It's a patchwork that can span multiple social media sites and news channels. It requires, as Henry Farrell and I have postulated, thinking of democracy itself as an information system. Disrupting an information operation will require more than disrupting one step at one time. The parallel isn't perfect, but it's a taxonomy by which to consider the range of possible defenses.

This information operations kill chain is a work in progress. If anyone has any other ideas for disrupting different steps of the information operations kill chain, please email me. I will update this in a future essay.

Bruce Schneier

Read More

Bruce Schneier is an internationally renowned security technologist, called a "security guru" by the Economist. He is the New York Times

best-selling author of 14 books — including "Click Here to Kill Everybody"—as well as hundreds of articles, essays and academic papers.

}